

REMARKS

The above amendments and following remarks are submitted in response to the official action of the Examiner mailed May 4, 2005. Having addressed all objections and grounds of rejection claims 1-20, being all the pending claims, are now deemed in condition for allowance. Entry of these amendment and reconsideration to that end is respectfully requested.

Claims 3-5, 8-10, 12-15, and 18-20 have been rejected under 35 U.S.C. 112, second paragraph. In response thereto, Applicants have herewith amended claims 3, 8, 12, and 18. Applicants wish to thank the Examiner for pointing to this issue. It is clear from the specification and drawings that the "special field" as disclosed and claimed is transferred with the "site identifier" and not with the "service request".

Claims 1-4, 6-8, 11-14, and 16-18 have been rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,275,939, issued to Garrison (hereinafter referred to as "Garrison:") in view of the article entitled "Access Control in Federated Systems" by De Capitani di Vimercati et al (hereinafter referred to as "De Capitani di Vimercati") and further in view of U.S. Patent No. 6,282,175, issued to Steele et al (hereinafter referred to as "Steele"). In response thereto, Applicants have amended all pending claims to specifically require a "manager" utilizing the claimed "administration module" to select the

appropriate security level for any given service request. Support for these amendments are found throughout the specification and drawings, with particularly detailed disclosure given in Figs. 11-12, along with accompanying discussion in the specification at pages 35-37. This ground of rejection is respectfully traversed as to the amended claims from the reasons provided below.

In previous responses, Applicants have presented substantial evidence and arguments regarding the failure of the Examiner to meet his burden under MPEP 2143 to establish a *prima facie* case of obviousness. Specifically, Applicants have shown that the Examiner has not shown motivation because the references teach against the alleged combination. In his response at page 21, paragraph 36, of the pending official action, the Examiner attempts to make his argument stating:

....since (sic) the alternative would be to impose local authentication, wherein users are required to re-authenticate themselves at each local site....

Applicants do not believe that this is found anywhere in the Examiner's citation or elsewhere in the reference. However, even if this teaching were found in the alleged combination, it explicitly teaches away from Applicants' claimed invention, because Applicants specifically does "impose local authentication". Furthermore, Applicants teach that this "local

"authentication" is preferable to a transfer of the user identifier over the public network as found in the prior art.

Furthermore, the Examiner has previously failed to make any showing of reasonable likelihood of success as specifically required by MPEP 2143. Instead, he has responded at page 22, paragraph 37, of the pending official action, stating:

Thus, an ordinary artisan can reasonably be expected to successfully incorporate a feature from one software product into another software product.

This statement is clearly erroneous, because it does not account for differences in hardware, software, and system architectures. Most simply, when one purchases a software package, the labeling typically lists "system requirements". In other words, that software package cannot be run on a given system unless it comports with those "system requirements". For more complex "real time" applications, differences in hardware, software, and system architectures become critical.

Specifically, amended claim 1 now requires:

an administration module located within said data base management system for permitting a manager having authority to access said administration module to associate a particular security level which each of said plurality of service requests

The Examiner admits that the alleged combination does not explicitly teach the limitation of "an administration module".

In rejecting claim 1, he states:

....wherein the existence of the security profile renders the claimed administration module inherent,

since (sic) the only claimed functionality if (sic) the administration module is to maintain the security profile, and the reference teaches the maintenance of a security profile at col. 7, lines 50-67 and col. 10, lines 5-17.

Clearly, the Examiner admits that the alleged combination does not have these further limitations. Furthermore, to find inherency under MPEP 2112 requires the Examiner to show that the reference "must of necessity" contain this entire limitation. Surely, he cannot. Therefore, the rejection of claim 1, and all claims depending therefrom, is respectfully traversed for failure of the Examiner to present a *prima facie* case of obviousness as required by MPEP 2143.

Claim 6 is an independent apparatus claim. Applicants have herewith amended it to contain:

an administration module located within said data base management system which may be utilized by a manager having authority to access said administration module to assign a particular security level to each of said plurality of service requests;

The alleged combination does not meet this limitation as explained above. Therefore, the rejection of claim 6, and all claims depending therefrom, is respectfully traversed for failure of the Examiner to make a *prima facie* case of obviousness as specified by MPEP 2143.

Claim 11 is an independent method claim having seven steps as amended. The added step involves "requesting said first

identifier from said user terminal". Not only is this step not found in the alleged combination, the Examiner admits:

....whereby all users accessing a database from a particular site are granted access.

The alleged combination does not have this step. Therefore, the rejection of claim 11, and all claims depending therefrom, is respectfully traversed for failure of the Examiner to make a *prima facie* case of obviousness as specified by MPEP 2143.

Claim 16 is an independent apparatus claim having means-plus-function limitations. Claim 16 has been amended to add the further element, "providing means located within said offering means for providing an authorized manager to assign a particular security level to each of said data processing services". As explained above, this element is not found in the alleged combination. Therefore, the rejection of claim 16, and all claims depending therefrom, is respectfully traversed for failure of the Examiner to make a *prima facie* case of obviousness as specified by MPEP 2143.

In his rejection of claim 2, the Examiner states:

Regarding claim 2, **Garrison** additionally teaches a data processing environment wherein a security profile is generated by said data management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

This finding is clearly erroneous. The Examiner's citation says nothing of a "security profile" and certainly says nothing of how

any security codes are "generated". Having previously pointed this out to the Examiner, he now holds:

....storing information defining what data is accessible to which users, the existence of which renders its generation inherent.

This finding does not comply with the requirements of MPEP 2112 for a finding of inherency, because the claim requires that the claimed "security profile" be generated by the data base management system. Because a data base management system stores a quantity does not mean that the data base management system has generated that quantity. In fact, most data base management systems simply store data which is generated elsewhere. The rejection of claim 2 and any claim depending therefrom is respectfully traversed as based upon clearly erroneous findings of fact and failure to comply with MPEP 2112.

Claims 3, 8, 12, 13, and 18 require a particular service request to include a site-specific user-id. Contrary to the Examiner's clearly erroneous findings of fact, Garrison separates client authorization and data retrieval into two separate functions (see for example Fig. 4A). The request for data (element 126 of Fig. 4A) is not transmitted by the client until password verification (element 117 of Fig. 4A).

In Applicants' claimed invention, the site-specific user-id must be transferred with the service request to impart greater granularity of security profiling. A given user may be

authorized to make certain service request but not others. In general, most users will not be authorized to make all service requests. The rejection of claims 2, 8, 12, 13, and 18 is respectfully traversed as based upon clearly erroneous findings of fact.

Claims 4, 14, and 17 depend from claims 3, 13, and 16, respectfully, and further limit the publicly accessible digital data communication network. As such they each present new and unique combinations not found in the prior art of record. The rejection of claims 4, 14, and 17 is respectfully traversed.

Claim 7 depends from claim 6 and is further limited by "wherein said terminal accesses said data base by transferring said service request to said data base management system". The Examiner cites Garrison column 6, line 60, through column 7, lines 32, and column 7, line 50, through column 8, line 37. Neither of these citations has even mentions a "service request". Though the term, "service request", has standard usage in the art, a working definition is provided by Applicants at page 25, lines 11-16, as:

The service request itself is utilized by Cool ICE service handler 156 to retrieve a previously stored sequence of data base management system command statements from repository 166. Thus, in the general case, a single service request will result in the execution of a number of ordered data base management system commands. The exact sequence of these commands is defined by the service request developer as explained in more detail below.

The rejection of claim 7 is respectfully traversed as based upon clearly erroneous findings of fact.

Claims 5, 9, 10, 15, 19, and 20 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Garrison in view of De Capitani di Vimercati in view of Steele and further in view of "UNISYS CSG MarketPlace - The Mapper System" (hereinafter referred to as "UNISYS"). This ground of rejection is respectfully traversed for failure of the Examiner to present a *prima facie* case of obviousness as required by MPEP 2143.

None of Garrison, De Capitani di Vimercati, nor Steele mentions a "data base management system". Therefore, it makes no sense to allege that one of skill in the art would be motivated to combine the teachings of UNISYS to provide a particular data base management system. Lacking motivation, it is extremely apparent that there is no reasonable likelihood of success of the alleged combination without the teachings of Applicants. The rejection of claims 5, 9, 10, 15, 19, and 20 is respectfully traversed for failure of the Examiner to make a *prima facie* case of obviousness.

Having thus responded to each objection and ground of rejection, Applicants respectfully request entry of this amendment and allowance of claims 1-20, being the only pending claims.

Please charge any deficiencies or credit any overpayment to  
Deposit Account No. 14-0620.

Respectfully submitted,

Paul S. Germscheid, et al

By their attorney,

Date August 4, 2005

  
Wayne A. Sivertson  
Reg. No. 25,645  
Suite 401  
Broadway Place East  
3433 Broadway Street N.E.  
Minneapolis, Minnesota  
55413  
(612) 331-1464